

RECEIVED
CENTRAL FAX CENTER
NOV 03 2006

Amendments to the drawings,

There are no amendments to the Drawings.

RECEIVED
CENTRAL FAX CENTER
NOV 03 2006

Remarks

Status of application

Claims 1-78 were examined and stand rejected in view of prior art. The claims have been amended to further clarify Applicant's invention. Reexamination and reconsideration are respectfully requested.

The invention

The present invention provides a system including methodologies for automatically detecting when a computer or device is plugged into a new network (or subnet). The system enables the user of the computer or device to decide whether or not he or she wants to permit the new network to be included as part of a trusted zone (i.e., a group of computers and devices amongst which information is exchanged relatively freely). Alternatively, the decision to include or exclude a newly identified network can be made by a previously established policy adopted by the user or an administrator. The system also automatically reconfigures a firewall to include or exclude the new network from the trusted zone.

The system first detects a connection to a new network by receiving notice of changes to an existing network configuration and evaluating these changes. Next, the new network is profiled and an identity is generated for the new network. The process of profiling a network involves collecting a number of items of information about the network in order to uniquely identify that specific network. This profiling process enables the system to generate a unique identifier for the network. Once a network has been identified, a user may elect whether or not that network is to be included as part of his or her trusted zone. Alternatively, the decision about whether or not to include a network as part of a trusted zone may be determined by a policy established by a system administrator or user. The new trusted zone definition, which either includes or excludes the new network, is automatically sent to the firewall for enforcement. The profile of each network is stored so that the next time the device is connected to the same network it will remember the network and apply the same security settings previously adopted for that network. The stored profile also facilitates the detection of changes to the network configuration or the connection of the device to a new network.

The system also includes configuration options that permit a system administrator or user to pre-configure the security settings of each system to identify networks that are part of the trusted zone. The system administrator or user may also pre-configure the system so that all unknown networks will be automatically excluded from the trusted zone.

Applicant's Information Disclosure Statement

Applicant electronically filed an Information Disclosure Statement (IDS) on November 21, 2003, a copy of which is attached herewith (as downloaded from the Office's PAIR system). As a signed copy of Applicant's IDS was not returned with the present Office Action, it is respectfully requested that the Examiner consider the art listed in the IDS, and return a signed copy of the IDS acknowledging that the listed art was considered.

Prior art rejections

A. Section 102 rejection: Bonn

Claims 1-19, 21-23, 25, 27-60, 62, and 64-78 stand rejected under 35 U.S.C. 102(e) as being clearly anticipated by Bonn et al., U.S. Pat. No. 6,738,908, hereinafter "Bonn". The Examiner's rejection of these claims is as follows:

As pre claims 1-19, 21-23, 25, 27-60, 62, and 64-78 Bonn '908 teach a generalized network security policy templates for implementing similar network security policies across multiple networks comprising: a client device/network element or Network security device "NSD" to regulate access to different networks, obtaining information to identify a particular client device, adapter /Ethernet cards, networks, generate a network profile, a current network profile, comparing profiles to determine if said device previously connected to current network, and if so applying security settings, determining and applying security settings to be applied (if new), storing and automatically applying when clients connects, applying established security policy/profiles, trusted and un-trusted

networks/trusted/optional- trusted to an extent external-un-trusted, obtaining user input for security profiles, a default security setting template /minimal template, setting for firewalls, identifying initial connections /new networks, a particular device configurations, a client, all network adapters, operating kernel /OS and memory a connection method / network IP, connection name / alias, gateway, private or public address, assigning a unique identifier to a profile/template or policy (abstract, figs. 1-5, 15-18, background, and summary et seq., col. 2, lines 4-45 et seq., col. 3, lines 53-63, col. 4, lines 6-15 et seq., col. 4, lines 23-27 et seq., col. 4, lines 64-67 et seq., fig. 2, figs. 1A and 1 B, col. 4, lines 38 et seq., col. 3, lines 60 et seq., fig. 15, col. 8, lines 1 -10 et seq., col. 8, lines 5-15 et seq., col. 1, lines 50 et seq., col. 6, lines 44 et seq., fig. 17, col. 8, lines 55 et seq., claims 1-8, fig. 4).

As discussed below, Applicant's claimed invention may be distinguished on a variety of grounds.

Bonn's teaching is directed to a template-based approach for expediting the deployment of security policies. There, the basic notion is to use policy "templates" that comprise network security rules specified with respect to one or more aliases. In other words, Bonn's basic approach is to allow the generic elements of a network (e.g., mail host, printer, etc.) to be described in terms of alias descriptors or roles, instead of specific IP addresses, so that fairly generic templates having preconfigured rules may be used (in a manner that is more expedient than configuring similar networks over and over again from scratch). The rules themselves are specified in terms of specific network elements, such as user workstations, servers, routers, and printers, which perform certain functions, or "roles." For example, a rule in a network security policy for a particular network may specify that all email traffic must flow through a network element having a particular network address that is specifically configured as a mail host (i.e., "MailHost" alias). By using a template that contains rules expressed in terms of aliases or roles, rather than in terms of specific network elements, Bonn's template-based approach provides a more efficient solution for configuring similar networks, rather than simply creating individual

policies that are similar entirely from scratch.

To generate a policy for a particular network from a template, Bonn's facility uses a profile of the network that maps the aliases occurring in the template to specific network elements within the network. For example, the network profile for a particular network maps the "MailHost" alias to a particular network element of the network having a particular network address (i.e., IP address). The facility uses the profile for the network to replace occurrences of aliases in the template with the addresses of the corresponding specific network elements.

Although Bonn's template-based approach undoubtedly is more efficient than configuring the same or similar networks over and over again from scratch, Bonn's approach does not include automatic detection of disparate networks (which may in fact be very dissimilar), and automatic firewall reconfiguration thereof, as a given device (e.g., laptop computer or other mobile device) is physically moved from one network (e.g., corporate network) to another (e.g., home network, or hotel wireless network). Instead at this point (i.e., at the point of generating a profile for a network), Bonn's facility simply provides a user interface where the user himself or herself must specify that a particular network is a "new" network and that it should have a particular profile (e.g., that the computer at IP address of so-and-so should be assigned the role of "MailHost"). Importantly, Bonn's facility has no means for the automatic detection or discovery of new networks as a given machine (especially, a mobile computing device) is moved from one network connection to another. As Bonn lacks this key feature of Applicant's invention, Bonn's described facility cannot re-create Applicant's solution, as set forth in Applicant's claims.

In order to understand this basic difference, it is worthwhile to review in further detail the specific problem addressed by Applicant's invention, as well as reviewing how Bonn's templates fail to provide any solution for that problem. Today, an increasingly large number of business and individual users are using portable computing devices, such as laptop computers, that are moved frequently and that connect into more than one network. For example, many users now have laptop computers that are plugged into a corporate network during the day and are plugged into a home network during the evening. The number of mobile computing devices, and the networks that they connect

to, has increased dramatically in recent years. In addition, various different types of connections may be utilized to connect to these different networks, such as 802.11 and Bluetooth. Wireless networks often have a large number of different users that are occasionally connected from time to time. Moreover, connection to these networks is often very easy, as connection does not require a physical link. Wireless and other types of networks are frequently provided in cafes, airports, convention centers, and other public locations to enable mobile computer users to connect to the Internet. Thus, it is becoming easier for users to connect to a number of different networks from time to time through a number of different means.

In this mobile environment it is very desirable for a user to be able to distinguish between the various networks and devices to which he or she is connecting. For example, if a user is at home, he or she most likely wants to allow very open communication with other home computers and devices. On the other hand, if the user is staying in a hotel, he or she would typically prefer much more limited communication with other computers and devices in the hotel. In this highly mobile environment described above, a significant problem is that many local networks use the same range of internal IP addresses (e.g., 10.10.x.x, 192.168.x.x, 172.x.x.x, etc.). As a result, mobile machines connecting to various different addresses cannot rely solely on IP addresses and subnet masks to identify a network or the machines and devices residing on the network. Applicant's invention addresses this problem by providing a solution that automatically discovers or detects new networks that a given mobile computing device connects to, and automatically reconfigures the device's firewall so that it may continue to receive protection from network threats (e.g., intrusions, attacks, viruses, spyware, and the like).

Bonn's focus, on the other hand, is the creation of his templates so that similar networks may be configured as to their generic (similar) network elements (e.g., generic rules for mail server, for FTP server, for Web server, etc., as such elements are common to many networks). Bonn does not, however, provide automatic detection and configuration of networks, as required by Applicant's patent claims. This point is made obvious by tracing through the user operation of Bonn's facility, as described in the Bonn patent. At the outset, the Bonn facility does not automatically detect new networks. Instead, the user must manually provide user input to identify a new network for the

Bonn facility, and in fact manually configure that network down to individual IP address.

Consider Bonn's Figs. 17-22, which show the configuration of a new network security device. In the dialog box shown in Bonn's Fig. 17, the Bonn user must first manually select "network security device configuration item 1712 and then selects Okay button 1720." (Bonn at col. 8, lines 55-59.) Then, the Bonn user must proceed to the dialog box shown in Bonn's Fig. 18 to manually select "a template for configuring the new network security device." (Bonn at col. 8, lines 60-67.) Now, the Bonn user must proceed to the dialog box shown in Bonn's Fig. 19 to manually instruct the system to generate a network profile (i.e., a list of aliases for specific network elements that are to be protected). However even at this point, the Bonn facility has not automatically mapped the template to the new network. Instead, the Bonn user must manually invoke "Edit button 1924 for mapping the aliases in the alias list to specific network elements within the network protected by the new network security device. In order to do so, the user selects each of the aliases 1921-1923 in turn, selecting the Edit button 1924 to define each." (Bonn at col. 9, lines 1-10.) Upon invoking the Edit button 1924 in Bonn's facility, the dialog box shown in Fig. 20 is displayed whereupon the user must manually match addresses for defining aliases in the user-created network profile. For example, to match up the alias and rule for an internal Web server (alias equal "InternalWebServer"), the Bonn user must manually enter a specific network (IP) address (address 2115) in the dialog shown in Fig. 21 (Bonn at col. 9, lines 22-26). As shown above, configuration of a network using the Bonn facility is hardly automatic, but instead requires the Bonn user to perform many manual steps, including specifying what network (IP) address goes with a given alias. At best, Bonn provides a facility that may be characterized as manual configuration of a network/firewall, with some efficiency gains provided by starting with generic templates (i.e., ones having predefined rules for common network elements, such as mail server, FTP server, Web server, and the like).

Applicant's invention provides the means for a mobile computer to dynamically reconfigure the computer's firewall as that device is plugged into each network. Note in particular that a user cannot use the Bonn facility to re-create this functionality. For example, if the Examiner were to take a work laptop computer (e.g., configured for PTO internal network) home (e.g., for connection to an ISP, such as AOL or Earthlink), the

Examiner could not rely on the Bonn facility to automatically identify and reconfigure the laptop computer for the new network (home) connection. Instead, if the Examiner were to rely on the Bonn facility, he would first have to manually identify the network to the Bonn facility (i.e., in accordance with the Bonn user interface shown at Figs. 17 and 18). Next, the Examiner would have to complete a sequence of manual user input steps (Bonn user interface, at least using dialogs shown at Figs. 19-21), for selecting a particular template to use and for mapping addresses of network elements on the Examiner's home network with aliases provided by the selected template. And in fact, a template suitable for a home network may not exist, whereupon the Examiner would have to expend additional effort first creating a suitable template. As should be readily apparent, the Bonn user is typically a system administrator or other individual with a working knowledge of networks and network addresses. One could hardly expect the average computer user to know how to assign IP addresses of various network elements to aliases in a template-generated Bonn network profile.

Turning now to the claims, one finds many differences between Applicant's claimed invention and Bonn's facility; for example, Applicant's network profile provides an identification means (e.g., based on MAC identifiers), whereas Bonn's "network profile" is really a merging of his template aliases with network addresses (e.g., IP address of 220.15.23.97 assigned to "InternalWebServer" alias). Nevertheless, deference is given to the Examiner's interpretation that the claims could be broadly interpreted to overlap with Bonn's described facility. Therefore, the claims have been amended to clarify that Applicant's claimed system and method automatically (i.e., without requiring manual user input) identifies and reconfigures devices for new network connections. For example, amended claim 1 now reads (shown in amended form):

1. (Currently amended) A method for a mobile client device to regulate access to different networks that the client device may be connected to, the method comprising:
automatically obtaining information to identify adapters connected to a particular client device and networks to which said adapters are connected;

automatically generating a profile for each network, including a current network to which said particular client device is connected;
automatically comparing said profile of said current network to previously generated profiles to determine if said particular client device has previously connected to said current network; and
if said particular client device has previously connected to said current network, automatically applying security settings previously utilized for said current network for regulating access to said current network.

(Applicant's other independent claims have been amended in a like manner.) As shown, the amended claim language explicitly requires Applicant's method to automatically detect new networks and automatically reconfigure the device's security settings/firewall -- all without requiring manual user input. (As an optional feature, the user is allowed to intervene in the process, if he or she desires, but the user's participation is entirely optional and is not required to implement Applicant's invention.) The user input required in Bonn's user interface (Bonn's Figs. 17-22) teaches, if anything, away from Applicant's automated detection/dynamic reconfiguration approach.

It is respectfully submitted that Applicant's claims, particularly in light of the foregoing amendments and clarifying remarks, set forth a patentable advance in the area of security/firewall management for mobile devices. Thus, it is believed that the amended claims distinguish over Bonn and that any rejection under Section 102 is overcome.

B. Section 103 rejection:

Claims 20, 24, 26, 61, and 63 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Bonn (above), as applied to claims 1-19, 21-23, 25, 27-60, 62, and 64-78 above, and further in view of the Examiner's taking of official notice. Here, the Examiner repeats his rejection based on Bonn, but adds official notice for the purpose of characterizing Applicant's network profiles. The claims are believed to be allowable for at least the reasons described above (under the Section 102 rejection) regarding the

deficiencies of Bonn. The claims are also believed to be allowable for the following additional reasons.

As described above, Applicant's system creates a profile for each network, which essentially serves as a fingerprint or identifier allowing Applicant's system to "memorize" networks that have been previously encountered. In this manner, when a user's mobile device is switched from one network to another (e.g., switch from a corporate network to a user's home network), Applicant's system can immediately and automatically identify previously encountered networks. This fingerprint or unique profile is based on information that is guaranteed to be unique, such as MAC identifiers (which are guaranteed to be unique across all networks). Bonn's network profile, on the other hand, simply refers to the mapping between template aliases and manually specified (i.e., user-specified) network addresses. Importantly, as Bonn provides no description about how to uniquely fingerprint or identifier different networks -- including, for example, no mention of the use of MAC identifiers -- it is doubtful that Bonn's facility could address the basic problem that stems from the fact that IP addresses of machines and devices on local networks are not unique and, in fact, are frequently duplicated on other networks. Applicant's invention solves this problem. Bonn's facility cannot solve this problem, as his facility makes no effort to ID networks at a finer level of granularity (e.g., based on MAC identifiers).

Accordingly, it is respectfully submitted that these claims distinguish over the cited art. Particularly in view of the foregoing amendments and clarifying remarks, it is respectfully submitted that any rejection under Section 103 is overcome.

Any dependent claims not explicitly discussed are believed to be allowable by virtue of dependency from Applicant's independent claims, as discussed in detail above.

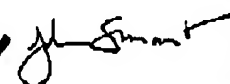
Conclusion

In view of the foregoing remarks and the amendment to the claims, it is believed that all claims are now in condition for allowance. Hence, it is respectfully requested that the application be passed to issue at an early date.

If for any reason the Examiner feels that a telephone conference would in any way expedite prosecution of the subject application, the Examiner is invited to telephone the undersigned at 408 884 1507.

Respectfully submitted,

Date: November 3, 2006

✓  Digitally signed by John A. Smart
Date: 2006.11.03 14:49:04 -0500

John A. Smart; Reg. No. 34,929
Attorney of Record

408 884 1507
815 572 8299 FAX



#2
12-5-03
JMY

Electronic Filing System (EFS) Data
Electronic Patent Application Submission
USPTO Use Only

EF5 ID: 51139
Application ID: 10003161
Title of Invention: System and Methodology for Automatic Local Network Discovery and Firewall Reconfiguration for Mobile Computing Devices
First Named Inventor: Gregor Freund
Domestic/Foreign Application: Domestic Application
Filing Date: 2001-11-14
Effective Receipt Date: 2003-11-23
Submission Type: Information Disclosure Statement
Filing Type:
Confirmation number: 7361
Attorney Docket Number: VIV/0004.01



RECEIVED

DEC 02 2003

Technology Center 2100


Total Fees Authorized:

Digital Certificate Holder: cn=John Allan Smart,ou=Registered Attorneys,ou=Patent and Trademark Office,ou=Department of Commerce,o=U.S. Government,c=US
Certificate Message Digest: 6e90a06a75f6724e4a60b2600d551d178c9b4277



TRANSMITTAL

Electronic Version v1.1
 Stylesheet Version v1.1.0

Title of Invention	System and Methodology for Automatic Local Network Discovery and Firewall Reconfiguration for Mobile Computing Devices	
Application Number: 10/003161  Date: 2001-11-14 First Named Applicant: Gregor Freund Confirmation Number: 7361 Attorney Docket Number: VIV/0004.01		
RECEIVED DEC 02 2003 Technology Center 2100		
<p>I hereby certify that the use of this system is for OFFICIAL correspondence between patent applicants or their representatives and the USPTO. Fraudulent or other use besides the filing of official correspondence by authorized parties is strictly prohibited, and subject to a fine and/or imprisonment under applicable law.</p> <p>I, the undersigned, certify that I have viewed a display of document(s) being electronically submitted to the United States Patent and Trademark Office, using either the USPTO provided style sheet or software, and that this is the document(s) I intend for initiation or further prosecution of a patent application noted in the submission. This document(s) will become part of the official electronic record at the USPTO.</p>		
Submitted by:	Elec. Sign.	Sign. Capacity
John Smart Registered Number: 34929	/s/ John A. Smart	Attorney
Documents being submitted us-ids	Files Submission-usldst.xml us-ids.dtd us-ids.xsl	
Comments		

0175 Jc-16
NOV 21 2003
PATENT & TRADEMARK OFFICE

ELECTRONIC INFORMATION DISCLOSURE STATEMENT

Electronic Version v18

Stylesheet Version v18.0

Title of Invention

System and Methodology for Automatic Local Network
Discovery and Firewall Reconfiguration for Mobile
Computing Devices

Application Number: 10/003161

Confirmation Number: 7361

First Named Applicant: Gregor Freund

Attorney Docket Number: VIV/0004.01

Art Unit: 2132

Examiner: Gilberto Barron Jr

Search string: (6550012 or 6269399 or 6233688 or 6233618
or 6141755 or 6075860 or 6065040 or 5987611
or 5881230 or 5875296 or 5864665 or 5857191
or 5838903 or 5832211 or 5828833 or 5815574
or 5764887 or 5740361 or 5623601 or 5603031
or 5602918 or 5588059 or 5586260 or 5557654
or 5475817 or 5434918 or 5241594 or 4914586
or 4295039).pn.



RECEIVED

DEC 02 2003

Technology Center 2100

US Patent Documents

Note: Applicant is not required to submit a paper copy of cited US Patent Documents

Init	Cite.No.	Patent No.	Date	Patentee	Kind	Class	Subclass
	1	6550012	2003-04-15	Villa et al.		713	201
	2	6269399	2001-07-31	Dyson et al.		709	224
	3	6233688	2001-05-15	Montenegro		713	201
	4	6233618	2001-05-15	Shannon		709	229
	5	6141755	2000-10-31	Dowd et al.		713	200
	6	6075860	2000-06-13	Ketcham		713	159
	7	6065040	2000-05-16	Mima et al.		709	202
	8	5987611	1999-11-16	Freund		713	201
	9	5881230	1999-03-09	Christensen et al.		709	203
	10	5875296	1999-02-23	Shi et al.		713	202
	11	5864665	1999-01-28	Tran		713	201

APP_ID=10003161

page 1 of 2

	12	5857191	1999-01-05	Blackwell et al.	707	10
	13	5838903	1998-11-17	Blakely et al.	713	202
	14	5832211	1998-11-03	Blakely et al.	713	202
	15	5828833	1998-10-17	Belville et al.	713	201
	16	5815574	1998-09-29	Fortinsky	713	153
	17	5764887	1998-06-09	Kelle et al.	713	200
	18	5740361	1998-04-14	Brown	713	201
	19	5623601	1997-04-22	Vu	713	201
	20	5603031	1997-02-11	White et al.	709	317
	21	5602918	1997-02-11	Chen et al.	713	153
	22	5588058	1996-12-24	Chandos et al.	380	279
	23	5586260	1996-12-17	Hu	713	201
	24	5557654	1996-09-17	Maenpaa	455	411
	25	5475817	1995-12-12	Waldo et al.	709	316
	26	5434918	1995-07-18	Kung et al.	713	169
	27	5241594	1993-08-31	Kung	713	151
	28	4914586	1990-04-03	Swinehart et al.	707	101
	29	4295039	1981-10-13	Stuckert	235	380

Remarks

Note: Remarks are not for responding to an office action.

This statement is not intended to represent that a search has been made or that the information cited in the statement is, or is considered to be, material to patentability as defined in Sec. 1.56.

Signature

Examiner Name	Date